WHITE PAPER
AUGUST 2018

IT@INTEL

Reduce IoT Cost and Enable Scaling Through Open Wireless Sensor Networks

Mats Agerstam
Principal Engineer, Intel IoTG

Robert Colby
Principal Engineer, Intel IT

Paul Donohue
Systems Integrator, Intel IT

Steven J Meyer
Sr. Principal Engineer,
Intel Manufacturing IT

Pranav Sanghadia
Senior Solution Architect, Intel IoTG

Executive Overview

For decades, operational technology (OT) and information technology (IT) enterprise groups have evolved their respective technologies and methods for handling business needs. On manufacturing floors, OT dominates due to its exceptional reliability, but IT excels at aggregating data for analysis and action. Manufacturing efficiency could greatly benefit from IT practices, but a range of issues inhibit adoption, including a general lack of open solutions in OT. Tied to this, wired sensor technologies dominate OT manufacturing environments, in part because there are currently no open, low-power wireless standards in the OT world.

This paper discusses a deployment project in which, based on simulations and lab analysis, we placed Bluetooth* Low-Energy (BLE) sensors with Intel® IoT Gateways in a live manufacturing environment. BLE is one of many open standard wireless technology options, and we detail several of our considerations, both pro and con, in weighing the top wireless options.

Additionally, we entered the project determined to answer a few key questions:

- Could our proof of concept network support at least 150 wireless nodes?
- Could wireless sensor battery life exceed 1.5 years in the field?
- Could our deployment's packet delivery achieve enterprise-class reliability in live manufacturing conditions?

We encountered some significant environmental challenges, but our results indicate that wireless sensor reliability exceeds 99 percent and, despite having attributes which might be improved in future deployments, is suitable for deployment in today's manufacturing environments.

Our results indicate that wireless sensor reliability exceeds 99 percent and is suitable for deployment in today's manufacturing environments.

Contents

Contributors

Shai Monzon
Engagement Manager, Intel IT

Acronyms

BLE	Bluetooth Low Energy
IoT	Internet of Things
LR-WPAN	Low-Rate Wireless Personal Area Network
MQTT	Message Queuing Telemetry Transport
OT	Operational Technology
OWSN	Open Wireless Sensor Network
PoC	Proof of Concept
QoS	Quality of Service
RF	Radio Frequency
TSCH	Time Slotted Channel Hopping

Challenges

Sensor networks are essential to "smart" IT environments (factories, buildings, data centers) and the legacy spaces of traditional industry that rely on operational technology (OT). Sensors monitor everything from environmental conditions to equipment statuses. However, the sensor networks' utility, cost, efficacy, and scalability vary tremendously.

Traditional OT wired sensor networks are closed, high-cost, proprietary systems that lack flexibility and interoperability. Modern IT offers a new way to address OT sensor needs with wireless sensor networks that are open, using commodity platforms and interoperability standards. Unfortunately, bridging the IT and OT worlds has historically been challenging. IT and OT have matured independently, and the market is only now bridging the two sides in ways that are affordable, compatible, and convenient.

Sensors collect data. When properly gathered and analyzed, that data can fuel preventative and predictive maintenance of equipment, leading to higher uptime, productivity, and final product quality. Ultimately, when it's time to execute, enterprise managers face the question of which sensors to deploy: wired or wireless?

Many wired sensors predominantly use Ethernet connectivity, a robust, predictable, and proven technology that offers the advantages (and challenges) found in conventional enterprise LANs. Moreover, power over Ethernet (PoE) allows wired sensors to be a single-cable solution, which simplifies deployment and management. However, Ethernet sensors can be costly, both on a per-unit capital basis and when adding units or changing sensor locations after site construction.

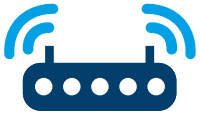
Wireless sensor networks typically cost a fraction of wired alternatives and, with no new wires to pull, are more convenient for retrofitting. Unfortunately, some impediments have dampened industry adoption of standard wireless networks in the OT space. Whereas Ethernet is the dominant industry standard for wired sensors, there is no such specification among Low-Rate Wireless Personal Area Networks (LR-WPANs, defined by IEEE 802.15.4), especially given the low-power, scalability, and security needs of enterprise and industrial environments. Vertical LR-WPAN specifications abound, but there are no open, horizontal, transport-agnostic specifications suitable for enterprise-wide deployment. Most current wireless solutions involve custom, proprietary infrastructures to connect a small set of sensors. Proprietary solutions can lead to vendor lock-in and siloed infrastructure, especially as businesses scale and new wireless sensor solutions tend to be incompatible with previous ones. This results in a redundant infrastructure with overlapping wireless radio gateways prone to radio interference. Further, such infrastructure is cumbersome to manage and expensive to deploy compared to open wireless alternatives.

Intel IT and Intel's Internet of Things (IoT) product developers have expanded on our existing work in horizontal IoT platforms[1] to research wireless sensor technologies that will help make IoT adoption more attractive in enterprise and industrial settings and bridge the gap between IT and OT.

Wireless Considerations

When running an Open Wireless Sensor Network (OWSN), there are many things to consider beyond data collection and transmission. The following discussion provides an overview of several such considerations.

Please note that these points reflect Intel's internal processes and thinking for this pilot project. They should not be considered general prescriptive guidelines. For a broad look at the qualities we feel are important in an OWSN suited to manufacturing environments, see the sidebar "What Makes an Open Wireless Sensor Network (OWSN) Enterprise-Ready?" later in this paper.



Challenges to creating a successful wireless sensor network might include:

- Distance between transmit and receive nodes
- Physical obstacles between nodes
- Interference from ambient wireless signals

Site Survey

Physical obstacles such as walls and metal structures can impede and scatter wireless radio signals. Some wireless technologies require line of sight between transmit and receive nodes, which can be difficult to achieve, especially in industrial settings. A possible solution is to adopt a radio technology with multiple-in, multiple-out (MIMO) capability, which uses asynchronous signals bounced off objects and walls. However, MIMO support may also drive up costs and require more power. (A wireless design, like tree mesh, may provide redundant paths and alternative routes for data around obstacles, which could be introduced after deployment.)

Physical placement of sensors can be critical to solution effectiveness since, especially in large environments, wireless signals inherently degrade over distance. Sensor placement can also contribute to latency and jitter, or packet delay in a data stream traveling to a receiver. As noted above, ambient wireless traffic can disrupt sensor signals, such as when Wi-Fi* streams crowd out Bluetooth* traffic.

During the planning phase we created a map showing distances, ambient interference levels, and other variables when deploying our wireless sensors and supporting APs. Of course, other factors must be considered, as well. For example, both the wireless technology and sensors themselves must be reliable for enterprise applications. The choice of appropriate wireless technologies and sensors is influenced by the type of industry or specific use cases, such as environments that impose restrictions on combustibles handling.

[1] Intel IT white paper, "Horizontal IoT Platform Paves the Way to Enterprise IoT Success"

Some of the likely candidates for Open Wireless Sensor Network include:

- Bluetooth Low Energy
- Bluetooth 5
- 5G
- IEEE 802.15.4 TSCH

Wireless Technology Options

There is no one-size-fits-all wireless technology for OWSNs. Every deployment needs to be analyzed to determine the best approach under given circumstances and priorities. The following are some of the likely wireless candidates.

Bluetooth Low Energy (BLE)

Currently in its version 4.2 iteration, BLE uses the same 2.4 GHz radio band as Classic Bluetooth and Wi-Fi standards such as 802.11b/g/n/ac. However, BLE uses 40 2-MHz channels rather than Classic's 79 1-MHz channels. Both standards use frequency-hopping to mitigate interference issues. This information helps support that BLE may be better suited to sensor applications in some of its performance specifications. BLE's maximum throughput is a fraction of Classic's (0.27 Mb/s versus 2.1 Mb/s), but connection latency is only 6 ms for BLE compared to Classic's typical latency of 100 ms. Moreover, BLE's power consumption is considerably less. Note that BLE is a single-hop technology, so if devices are out of radio range, there's no capacity for assisting node transmissions via a mesh topology.[2]

Bluetooth 5

Bluetooth 5 arrived in 2016 and is largely targeted at IoT implementations. Bluetooth 5 supports the older Classic specification but is more flexible. For example, nodes can double their normal burst speed (up to 2 Mb/s) in exchange for a shortened range. Conversely, nodes can quadruple their range if throughput rate is sacrificed. Unlike BLE, Bluetooth 5 supports mesh topologies, which can help extend range and resilience as well as enable self-healing networks. Bluetooth 5 also supports IPv6 over Low-Power Wireless Personal Area Networks (better known as 6LoWPAN). The 6LoWPAN specification allows Internet Protocol (IPv6) traffic to flow across IEEE 802.15.4-based LR-WPANs. In other words, IEEE 802.15.4 could be considered as a slower, low-power Wi-Fi that can operate via Bluetooth 5.

5G

5G wireless technology may be a poor fit in enterprise sensor network environment. 5G sends and receives data at high speeds over long distances, which consumes power more quickly than a low-energy approach would. More importantly, enterprises need their connections to be contained within controlled, secure boundaries. 5G, which sends all communications across the provider's cellular network, may not comply with an organization's security requirements.

[2] In some deployments, Bluetooth 4.x may be superior in performance over 5.0 and 802.15.4 TSCH – and vice versa. For example, in a low-density deployment, CSMA/CA will likely perform better than a time-synchronized network like 15.4 TSCH due to its periodic (every 30 seconds or so) network synchronization, which entails a constant background power consumption. As the number of nodes in the deployment scale, there will be a point where 802.15.4 TSCH will be more efficient due to the collision/retransmission overhead in CSMA/CA. Our solution architecture is designed to be flexible and modular, not imposing a single solution. For example, BLE sensors could be replaced with LPWAN sensors (BLE 4.x/5.0 or IEEE 802.15.4 TSCH). The least common denominator here is 6LoWPAN. MQTT is one option for data ingestion. Our system is designed to support others, including DDS, which is designed to be more scalable than MQTT, offering higher QoS, higher throughput, and no single point of failure due to its decentralized nature.

IEEE 802.15.4 TSCH

Time Slotted Channel Hopping (TSCH) arrived in 2012 as an addendum to the 802.15.4 standard. It provides for a time-synchronized network and network management that sends data across different channels at scheduled times. This method helps save power, because radios can be deactivated when not in use, and it performs well in problematic environments prone to data loss. IEEE 802.15.4 TSCH is centralized, distributed, and autonomous, making it compatible with tree mesh topologies. It also supports standard protocols such as 6LoWPAN.

Installation and Security Considerations

Some sensor networks are easier to install and manage than others, and many elements need to be considered during planning, for example, provisioning of both hardware and software. The convenience and complexity of this task depends on the tools available to help with registration in the central management server. This is another reason to pursue open, standards-based solutions: They provide greater flexibility in finding and/or customizing the best tools for specific environments and preferences.

Early in our proof of concept installation, we deployed a sample gateway and loaded it with various sensor nodes. This allowed us to confirm expected provisioning, power consumption, and performance levels without committing to a larger installation prematurely.

Similarly, consider edge aggregation. In our proof of concept (PoC), we connected sensor nodes to Intel® IoT Gateways,[3] which in turn relayed traffic to APs. Gateways should be user-friendly yet flexible and secure. Early in our PoC installation, we deployed a sample gateway and loaded it with various sensor nodes. This allowed us to confirm expected provisioning, power consumption, and performance levels without committing to a larger installation prematurely.

Physical security is also important. Are sensors and other devices equipped to be locked or affixed in place to prevent theft or accidental falling? In the case of hacking, an attacker could have physical access to the hardware. Security controls should mitigate this vulnerability through methods such as secure software boot-up, physical port disabling, defense against cloning, and data encryption. Additionally, if the environment involves moving equipment, are devices robust enough to be handled roughly without failing?

Proof of Concept (PoC)

Intel IT selected one of our own fabrication facilities as a proving ground for an enterprise-scalable IoT wireless network PoC. Our objective was two-fold: 1) to validate Bluetooth Low Energy (BLE) performance in a fab environment following simulations and lab measurements, and 2) to measure and validate power consumption of the PoC solution. This process would demonstrate the feasibility of a centralized, IT-managed wireless IoT platform, suitable for OT, integrated with a supervisory control and data acquisition (SCADA) back-end and an IT-approved device management solution.

[3] Intelligent Gateway Solutions for IoT, intel.com/content/www/us/en/internet-of-things/gateway-solutions

The following are the requirements we defined for the platform we are developing:

- Reusable and shareable "horizontal" solution that can work agnostically across a wide range of wireless technologies and sensors
- Adherence to industry networking standards
- Relative ease of deployment (sensor plug and play)
- High scalability and high density
- Enterprise-class quality of service (QoS) despite low-power constraints (minimum 1.5-year battery life) and challenging environmental conditions
- Shareable sensor datasets with common APIs to facilitate analysis among a broader base of systems
- Lower total cost than wired-only configuration
- Flexible deployment, meaning sensors are easy to relocate and reconfigure as needed

The last three of these are "soft" points that are difficult to quantify. However, as we will explain below, our testing established targets for most of these criteria, and our results can help refine more quantitative expectations going forward.

Figure 1 illustrates our basic concept of placing wireless sensors where needed in an enterprise environment, especially in industrial settings, and how those sensors convey data for analysis and action. When designing the PoC, we used existing Wi-Fi access points (APs), to minimize the introduction of parallel infrastructure. These Intel IoT Gateways then connected to APs that allowed us to maintain flexible endpoint management at the network edge, then transition to established wired/wireless infrastructure at various aggregation points. Our use of Intel IoT Gateways enabled us to pursue a common protocol between the sensor network and the northbound network from the gateway to an analytics cloud rather than be limited only to the protocols supported by our specific sensors.

The PoC success criteria should demonstrate that wireless IT/OT connectivity provides a variety of benefits:

- **Low cost.** According to our estimates, wireless sensors can deliver up to 90 percent capital expenditure savings compared to installing more wires and cables.[4] (We do not consider wireless sensors as a replacement for wired. Rather, wireless sensors will complement and augment the value of wired infrastructure, which will remain the de facto technology in mission-critical applications for the foreseeable future.)

[4] Maximum savings depend on the specific sensors deployed as well as the costs of retrofitting new wiring into place for wired options. If an organization has proactively installed extra Ethernet drops for future use during site construction, then those significant retrofitting costs do not apply, and savings adjust downward appropriately.

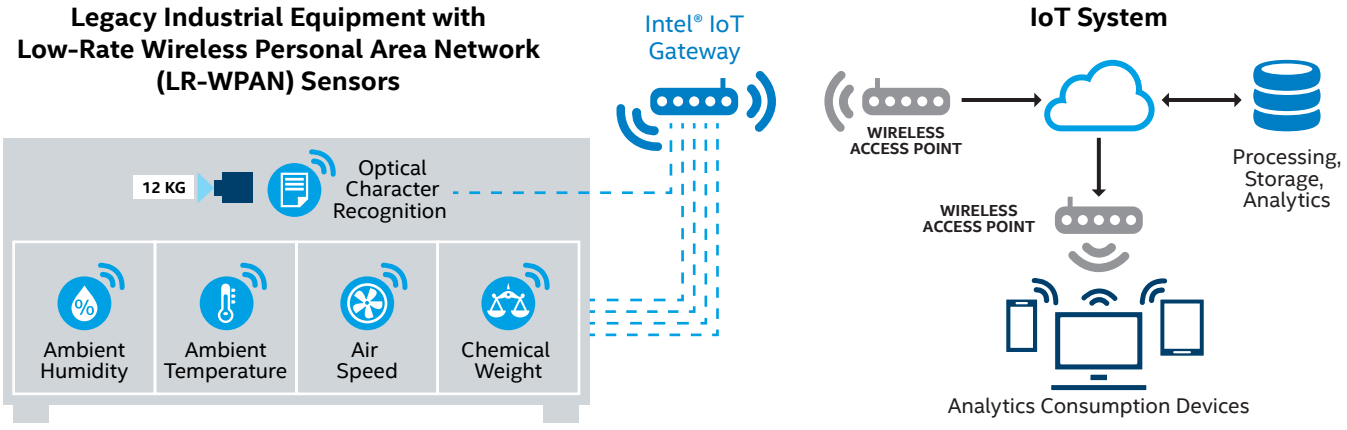


Figure 1. Example of an Internet of Things (IoT) wireless sensor system in an enterprise environment.

- **Greater time-efficiency.** Wireless sensors typically deploy in far less time than wired alternatives. Moreover, they respond to the changing demands of a complex manufacturing environment with more agility.
- **Flexible.** Wireless sensors provide mobility and can reach anywhere within the facility, including areas not covered by existing wired infrastructure. As noted, wireless approaches that are planned and deployed by IT help eliminate the costs of stringing new cables; hence, wireless creates a dynamic environment that can adapt to changing business needs.

We conducted our PoC in three stages: simulation, lab measurements, and pilot deployment. Our simulation studies focused on wireless performance and power consumption, as battery life is a core element in many wireless environments. Lab experiments targeted measurements that examined the impacts of radio interference on performance and corroborated expectations set during simulations. Lastly, PoC deployment (see the Results section) brought our platform into a real-world factory environment, where we could calibrate, optimize, and analyze our implementation.

Use Case

Earlier, we mentioned how smart wireless sensor networks could facilitate predictive maintenance. One example of this involved pressure monitoring of factory exhaust laterals. Monitoring helps to detect anomalies and identify problems within the exhaust system and also indirectly measures the health of factory tools. In fact, a 2015 analysis at Intel[5] estimated that real-time exhaust pressure monitoring at 400 critical points and the vibration monitoring of rotating mechanical equipment could yield a 50 percent reduction in production interruptions; power savings of 0.7 million kWh/year; 50 percent lower maintenance costs; and 2,500 hours of labor saved annually. Moreover, if exhaust laterals are not working properly, it can take longer to bring a fab online. However, while our PoC would not single-handedly pave the way to these benefits, its success may play an important role in guiding future efforts toward these benefits.

Within Intel's fab environment, exhaust lateral monitoring data was previously measured by someone walking out to each sensor and recording its readings. We did not want to add more wiring infrastructure to support automated data collection due to high total deployment costs. Our estimates show that each new wireless sensor would cost roughly 10 percent of a wired alternative.

Potential Use Cases

Exhaust lateral monitoring represents only an early application of Open Wireless Sensor Networks (OWSNs) for Intel. Intel is already looking at opportunities to place wireless sensors into pump systems, fans, and even robot arms. There are potentially thousands of applications, and, in many of these cases, wired sensors may be infeasible. Constant motion and wear of wired sensor cables on a moving robot could lead to premature failure. Wireless sensors can be beneficial on any machine with moving parts that could negatively impact production if the machine failed. Collectively, the benefits could add up to millions of dollars per factory.

We are also examining opportunities for wireless sensors in liquid monitoring. Often, chemicals used in a factory must be measured. Wiring may prove infeasible due to distances between these chemicals and facility infrastructure, especially power. Wireless sensors may be more affordable, and sensors can be placed exactly where needed.

Factory stockers may also benefit from OWSNs. Stockers have sensors, as do the robots that deliver materials to factory tools. Wireless sensor networks could help monitor stocker functionality and performance across several moving parts. If monitored characteristics fall outside of certain thresholds, corrective action can be taken before a stocker fails and production stalls.

Intel is also considering applying wireless sensors to factory ergonomics wearables. Wearable sensor systems can monitor employees as they work and provide instant feedback if they are not correctly following safety procedures. Managers can also receive this information and take near-real-time action to help employees avoid accidents and injuries.

[5] Intel 2015 Corporate Responsibility Report, csrreportbuilder.intel.com/PDFfiles/CSR-2015_Full-Report.pdf

Simulation

We investigated both network performance and sensor battery life in our simulations.

Network

We determined that our PoC should support at least a 150-node wireless sensor network. We used a software simulation to find out whether our BLE 4.2-based wireless infrastructure could handle this load.

Our simulations accounted for varying levels of QoS and their impact on a successful sensor report delivery. We also assessed various blocked channels and packet error rates (PER) (up to 5 percent) but not radio frequency (RF) propagation. Ultimately, we successfully simulated 150 nodes, but we only scaled to 80 nodes in lab testing, as this accounted for all of the sensors we had available.

Battery Life

It would be extremely difficult and inefficient to consistently replace batteries in thousands of factory sensors. Thus, our objective was to produce a solution that could run reliably in the field for a long period, which we defined as at least 1.5 years.

We calculated our sensor battery life based on manufacturer specs combined with expected transmit/receive (Tx/Rx) activity, plus idle mode energy consumption. However, outside the lab, actual power consumption depends on a wide variety of factors, from the type of sensor to the response time needed for a fault. Measurement polling intervals are also important, as is the number of sensors connected to each node. This degree of battery life accuracy estimation was beyond the scope of our PoC.

Table 1 shows results from our simulation of 150 sensor devices. It illustrates overall power consumption for a particular hardware sensor. In short, the data encompasses RF conditions across three BLE channels and corresponding PER. This data helps determine the overall lifetime of a device battery given different configurations of BLE behavior.

Given the power characteristics of our specific Bluetooth microcontroller unit (MCU) and our estimated traffic patterns, our expectation of approximately 4.5 years exceeded our battery life requirements (1.5 years). In our simulation, we did not account for the power draw caused by measurements taken from integrated or discrete sensors connected to the node; however, we did measure the power consumption of the wireless transceiver.

Table 1. Battery Life Data for Simulations

RF Conditions (# of Channels/Percentage)	3/0%	2/5%	1/5%	3/0%	2/5%	1/5%	3/0%	2/5%	1/5%	3/0%	2/5%	1/5%
Report Interval	60 seconds			10 minutes			30 minutes			60 minutes		
Beacon Packets	5	5	14	5	5	14	5	5	14	5	5	14
Advertisement Rate	125ms			125ms			125ms			125ms		
Reliability	99%	99%	99%	99%	99%	99%	99%	99%	99%	99%	99%	99%
Uniform Time Spread	400ms			4000ms			12,000ms			24,000ms		
Concurrent Sensors	2	2	5	1	1	1	1	1	1	1	1	1
Power Consumption (µA)	5.2	5.2	3.07	2.02	2.02	2.23	1.94	1.94	2.01	1.92	1.92	1.95

Packet Delivery

Figure 2 illustrates the overall probability for a successful delivery of a sensor report as a function of sending multiple identical report packets, one after the next, under different conditions. Sensors reported data in connectionless mode (so there was no way for the gateway to acknowledge that data was received by a particular sensor). Therefore, we needed to send an appropriate amount of beacons/reports to the gateway to reach a specific level of reliability. In this case, we used a maximum of 14 beacon frames. The details in Figure 2 demonstrate that under some of the worst radio conditions, we achieved more than 99 percent probability of success starting at just five beacon frames. The first frame could be successful, or the third, or the last; in some cases, all frames were successful. But only in 1 percent of the cases would all frames fail to be received successfully.

Lab Measurements

We compared the results of our simulation (150 simulated nodes) to those of our lab test (80 physical nodes). QoS data from our lab tests were very encouraging, showing results within 1 to 2 percent of our simulations.

We ran the lab tests in a controlled clean room. As with the simulations, we tested with varying QoS levels that could impact the probability of a successful sensor report delivery. Additionally, we tested with and without RF interference, intending to simulate worst-case conditions from ambient Wi-Fi interference. Specifically, we configured Wi-Fi traffic to operate on select channels interfering with the BLE advertisement channels, then we flooded those channels to capacity with UDP traffic using air-time inefficient MCS (Modulation and Coding Scheme) settings. This flooding saturated the spectrum used for BLE advertisements, causing the particular channel to be unusable. We varied the number of blocked Bluetooth advertisement channels as well as the uniform probability distribution function PERs, which we varied up to 5 percent.

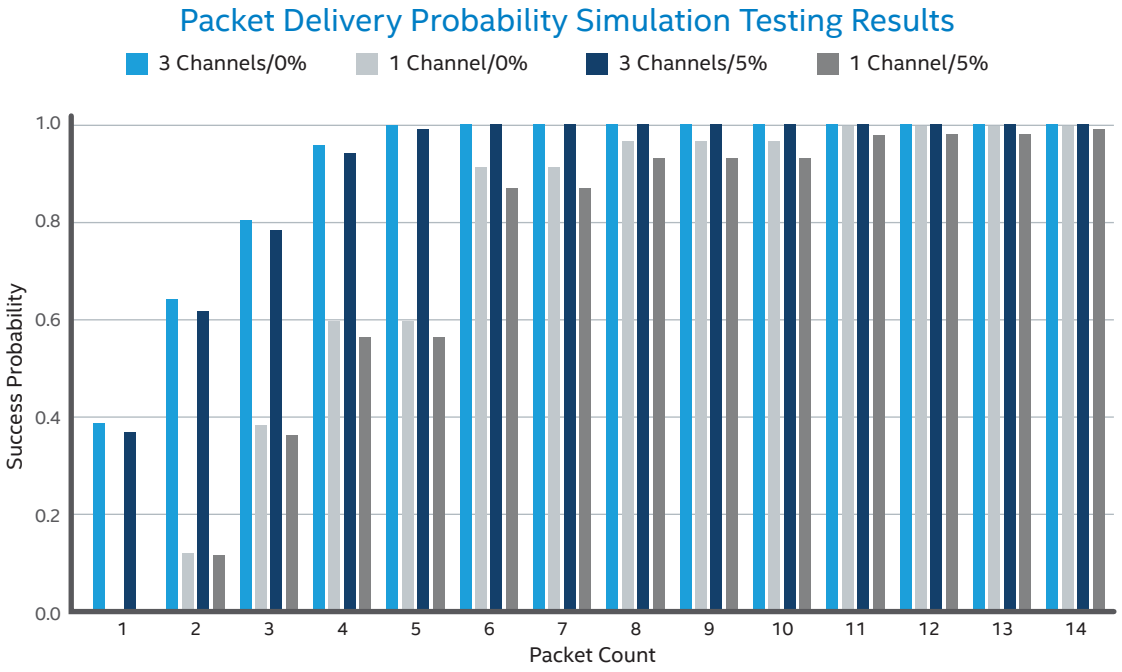


Figure 2. Overall probability for the successful delivery of a sensor report as a function of sending multiple identical report packets under different conditions.

What Makes an Open Wireless Sensor Network (OWSN) Enterprise-Ready?

We had one important question during planning process: What qualities should an Open Wireless Sensor Network (OWSN) have in order to meet the rigorous demands of our factory environment and, more broadly, enterprise environments as a whole? Every business and OSWN will have different needs, but we had some thoughts on common OWSN qualities that could be useful to future Intel endeavors:

- **Low power consumption.** Changing batteries is time- and labor-intensive, and the less it needs to be done, the more the organization will save on labor.
- **Coverage, range, density, and scale.** Enterprise environments can be large and/or cramped. Wireless sensor networks must be able to span potentially long distances and scale upward in quantity, as needed, without impairing the network's performance.
- **Quality of service (QoS).** Wireless sensor networks must maintain QoS, regardless of ambient interference, sensor quantity scaling, and other factors.
- **Traffic patterns/flows.** OWSNs need to adapt to dynamic environmental conditions that impact traffic characteristics, including data rate, latency, and jitter.
- **Resilience, failover, and self-healing.** Sensors fail sometimes. An OWSN should accommodate the unexpected, either through topology selection or other means.
- **Device authentication.** Every device on the network should be validated to ensure its ability to thwart the presence of rogue hardware and other security risks.
- **Encrypted communications.** All wireless traffic can be snooped. Encryption will help keep data safe.
- **Ability to perform updates.** OWSNs involve smart devices for increasingly smart environments. As such, they should be updateable, preferably through methods that are easy to push out and that can ensure update integrity.
- **"Wi-Fi*-like" qualities.** The following characteristics are related to the use of Wi-Fi:
  - **Ubiquitous infrastructure.** Typically, any Wi-Fi access point (AP) can be accessed from anywhere in the world. In enterprises, especially in operational technology (OT) settings, that ubiquity does not exist—yet. We predict that technologies such as IEEE 802.15.4 will soon remedy that.
  - **"Just works."** With ubiquity should come plug-and-play usability. Soon, we hope to see any off-the-shelf wireless sensor work with most OWSN deployments.
  - **Vendor agnostic.** Compliance with industry standards should help enable OWSNs to integrate third-party products.
  - **Device mobility.** As environments evolve, OWSNs should support the ability to move sensors.
  - **Secure.** Wi-Fi can achieve formidable security with just a few clicks. OWSNs should be the same.
  - **Simple—one or two radio standards with global availability.** Wi-Fi offers a common set of protocols on only two radio bands. OWSN technology can and should be similar.
  - **Low edge cost.** Ultimately, OWSNs will only become prevalent if they are affordable to deploy. Low technology costs coupled with high product volumes can help make this possible.

Solution Architecture

When deploying our platform in the real-world environment, we used a tree mesh architecture, as shown in Figure 3. This approach provides for ample scalability and straightforward management. The following are some of the components of our OWSN.

- Wind River Helix* Cloud, which provides a protocol for communicating between the gateway and the edge
- Intel IoT Gateways
- BLE sensors
- Message Queuing Telemetry Transport (MQTT) broker, which relays sensor data to subscriber devices
- Customer user interface, driven by common APIs and visualization tools for consuming data

Our solution architecture included the ability to publish sensor data in an open, standard way with MQTT. The MQTT protocol allows customers to subscribe from any data system they already have that is capable of such subscriptions. We are integrating this solution into existing factory SCADA systems using an MQTT listener.

Results

We were confident as we rolled out a real-world deployment of BLE 4.2-based sensor nodes. However, we did not have experience with the actual manufacturing environment. We did not know how much obstruction there would be between sensor nodes and gateways, the impact this would have on overall range, and how other environmental factors would impact our results.

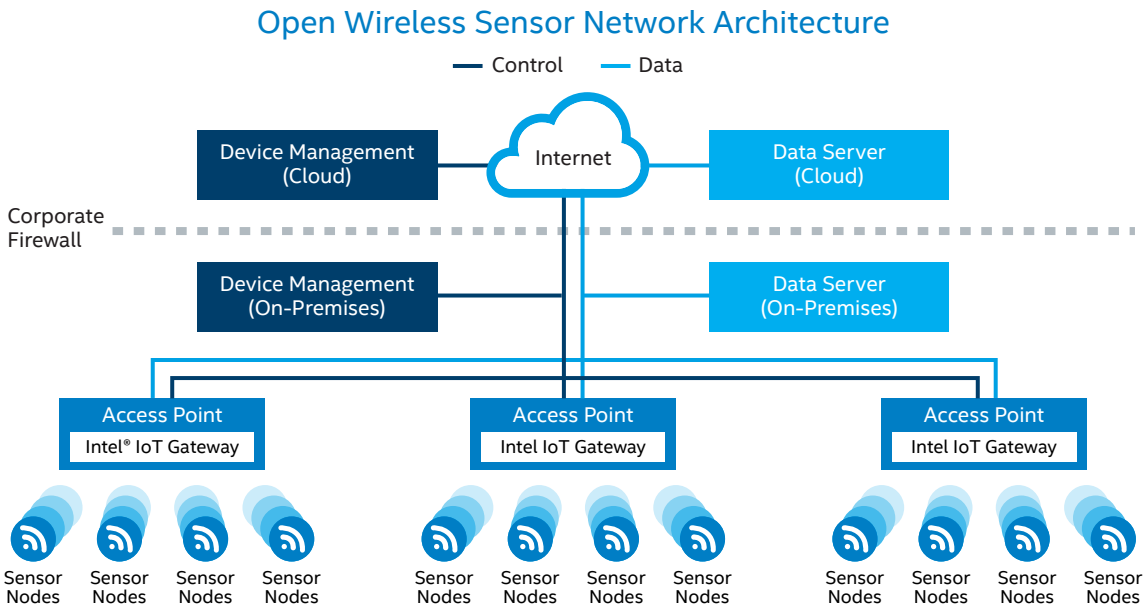


Figure 3. The tree mesh architecture that we implemented in our live environment emphasizes signal clarity and performance along with redundancy and the network's ability to self-heal.

Nevertheless, we remained confident enough to deploy with an even higher density of sensor nodes than we had modeled in simulations: 250 nodes rather than 150.

As illustrated in Figure 4, we encountered a higher number of concrete pillars and metal columns than expected, and adjacent manufacturing equipment also caused significant radio interference. Overall, although we anticipated an environment with fewer impediments, the results we achieved represent real-world challenges and accurate outcomes.

Over the ten-day evaluation period of the real-world deployment, we accumulated millions of data points. Although communications typically remain reliable up to 120 feet in office settings, we experienced high reliability overall at distances up to 90 feet in our test manufacturing environment. Figure 5 (on the next page) shows that more than 99 percent of sensor communications had high reliability; less than 1 percent were not reliable.

One issue that affected our reception of a wireless infrastructure was the lack of an external antenna on our BLE sensors, which limited our communication range. However, we chose this design based on the fact that it was the optimal solution that fit our time constraints in the quantity (250) we wanted.

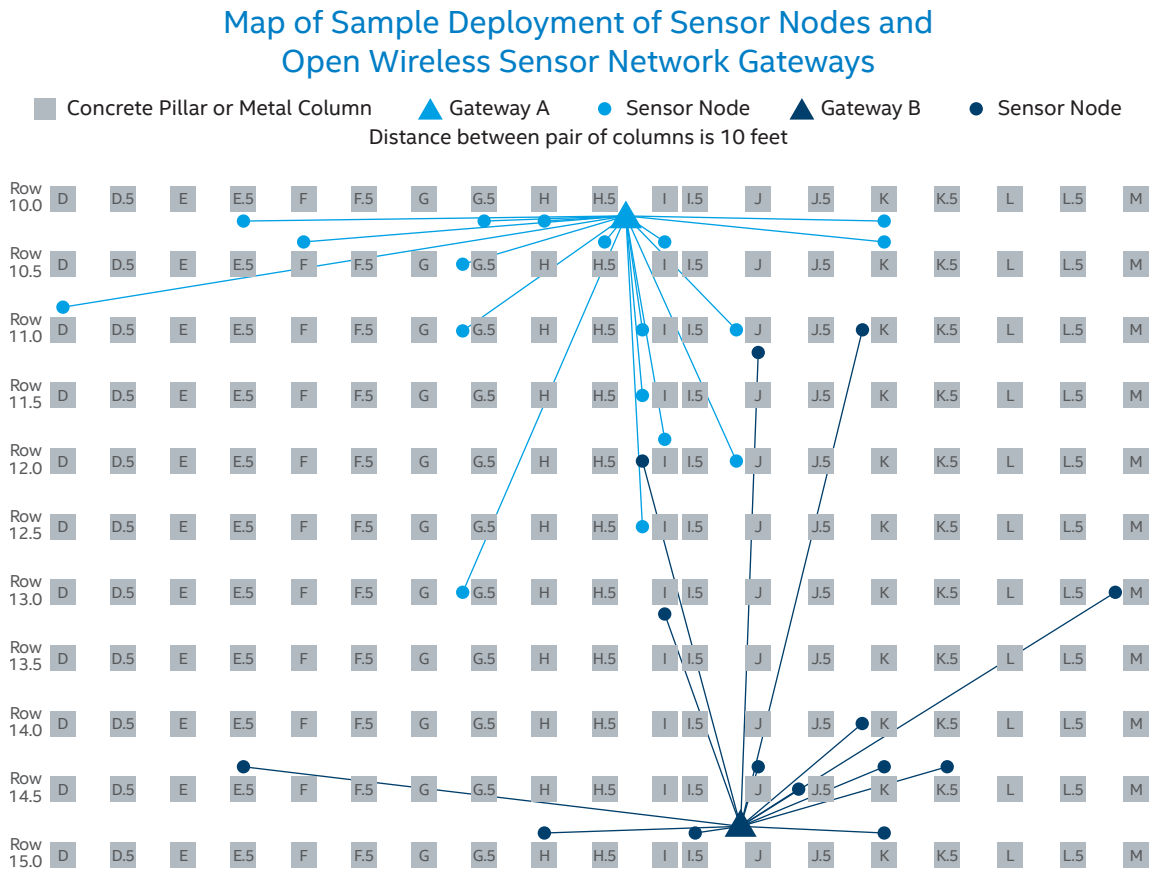


Figure 4. This map of Intel's sensor node deployment shows the challenges caused by concrete and metal obstructions on wireless receptivity across the fab's manufacturing environment.

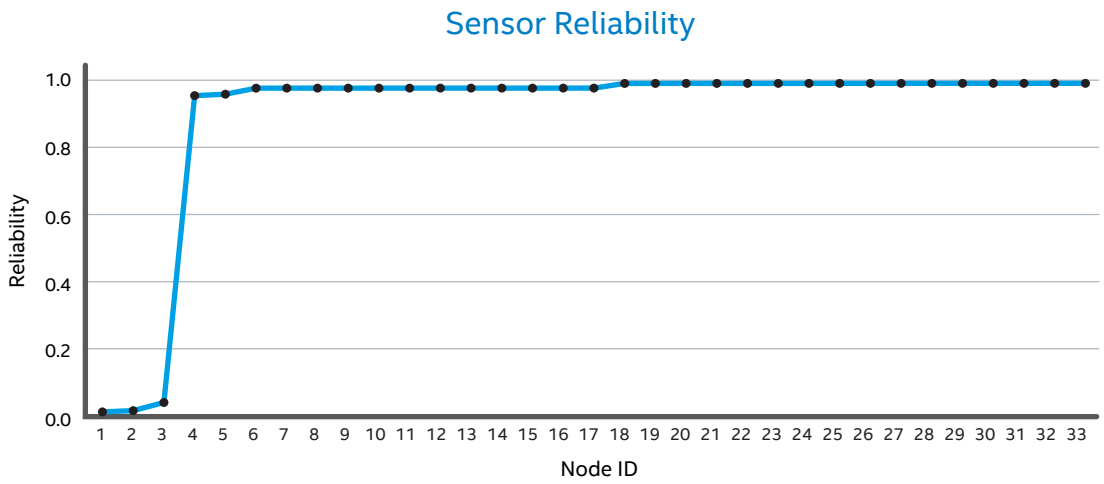


Figure 5. Intel engineers measured greater than 99 percent reliability, despite more aggressive over-the-air utilization with higher sensor counts. Results where reliability was poor almost invariably involved sensor-to-gateway distances at the edge of the sensor's range.

Table 2 shows the calculation of the power consumption for two different devices, both based on the same SoC. In the first configuration, idle power is not optimized; in fact, it outstrips active power draw. The second configuration shows a higher active power draw but a more appropriate idle mode. When all other factors remain constant across the two configurations, the impact on total battery life is substantial. Clearly, idle power configuration is critical in extending battery runtime—a key finding that will figure prominently in our subsequent wireless enterprise efforts and optimizations.

Our results demonstrated that a mesh of wireless sensors and Intel IoT Gateways could be easily deployed and reliably operated in a real-life manufacturing environment. We encountered obstacles including distance, obstructions, and ambient radio interference, but our solution demonstrated the ability to reliably manage these factors and maintain a predictable output stream of sensor data for centralized collection and analysis.

Table 2. Battery Life Data for Factory Floor Use

	Primo	HoneyPie
Advertisement Interval (14 frames)	125 ms	125 ms
TX Payload	31	31
Idle Power (µA)	220	20
Active Power (µA)	130	286
Active Time/ Hours	109	109
Inactive Time/ Hours	3491	3491
Battery Life	48 days (250 mAh)	452 days (620 mAh)

Next Steps

Earlier, we noted our issues with limited reception range. BLE 5 would offer a superior link budget compared to the BLE 4.x we deployed, allowing for higher transmission power. If the move to BLE 5 can double the transmission range, that would translate into quadrupling the coverage area and a corresponding drop in the number of needed gateways, which in turn would significantly lower total solution costs. Alternatively, a similar radio technology based on 900 MHz would cover longer distances than 2.4 GHz could and with less power consumption.

Another concern with our choice of using BLE 4.2 technology focused on multi-path propagation. The many obstructions that caused signal bounces and the diffraction from signals traveling through dense materials (such as concrete) created multiple instances of signals arriving at gateway receivers at different times. BLE uses windowing and channel-hopping techniques to help cope with multi-path, but BLE lacks multiple antennas, preventing receive diversity.

Most importantly, we learned that "working" nodes operate in a binary fashion—either on or off. We witnessed how a sensor at 86 feet from the gateway might regularly experience -50 dBm, then drop to -75 dBm for five hours before returning to normal. Over time, we learned from manufacturing staff that this variance was caused by the electro-magnetic noise generated by nearby equipment. Proactively considering these factors would allow for greater optimization in sensor and gateway placement, balancing higher reliability with environment-appropriate sensor density.

We will continue to look for ways to extend battery life of sensor gateways beyond the observed 452-day average, which might include:

- Reducing idle power consumption
- Additional battery resources
- Software to dynamically adjust number of beacons sent per hour

We did not have any concerns about reaching or exceeding the I/O limitations of our gateways, but we did complete the trial with the expectation that battery life would have lasted longer than the 452-day average we observed. We derived our finding by operating 250 nodes with a reporting interval of 10 minutes. This accelerated reporting time provided us with a "time lapse" view of battery use. At 452 days, this nearly met the requirements of Intel IT (1.5 years), but we will explore ways to extend battery life, particularly in lowering idle power consumption (which comprises 97 percent of the sensor's use). We might also consider using additional battery resources as well as software to dynamically adjust the number of beacons sent per hour depending on environmental conditions.

We want to verify that our OWSN platform(s) can easily adapt to any suitable, standard wireless technology. As the industry matures, many elements will be required to make a truly horizontal platform a reality. Among these are the development of a modular architecture with replaceable sub-components and possibly a new wireless standard designed to meet broad enterprise market needs.

Intel IT will continue to work with industry-standards bodies to develop and refine enterprise wireless solutions, particularly those that contribute to OT environments. We have been actively working with the Open Connectivity Foundation (OCF), the Industrial Internet Consortium (IIC), and others to expand this work in future Intel initiatives.

Conclusion

In the ongoing industry effort to bridge the worlds of OT and IT, wireless technologies are destined to play a pivotal role as a solution for both physical and cost challenges. Intel IT wants to assist in bridging OT and IT by facilitating open technologies and frameworks for mass adoption. Openness can lower cost barriers to adoption, help create a competitive marketplace to accelerate solution evolution, and enable businesses to more easily integrate solutions into their existing infrastructures.

In conducting the aforementioned simulation and deployment, we sought to prove that wireless sensors based on open technologies, such as industry-standard BLE and off-the-shelf sensor nodes, could provide wired-class reliability and interoperability with off-the-shelf gateways, such as the Intel IoT Gateway. At each step, we embraced solutions with the broadest industry adoption, interoperability, and support. We consider our efforts successful based on the results of greater than 99 percent reliability in sensor communications. Therefore, we would recommend this solution for non-critical systems in Intel factories. Critical systems, of course, are more sensitive to the reliability concerns inherent in wireless communications and will likely adopt wireless solutions more slowly.

As noted, there are several elements in our deployment configuration that can be updated, changed, and/or optimized. The advantage of using open technologies is that we can make such changes almost immediately. Intel IT is highly motivated to pursue these inquiries as a means toward improving organizational unity across OT and IT divisions as well as bolstering company-wide efficiency. If our tests and processes can serve as inspiration and methodology for others in the industry, so much the better.

For more information on Intel IT best practices, visit **intel.com/IT**.

IT@Intel

We connect IT professionals with their IT peers inside Intel. Our IT department solves some of today's most demanding and complex technology issues, and we want to share these lessons directly with our fellow IT professionals in an open peer-to-peer forum.

Our goal is simple: improve efficiency throughout the organization and enhance the business value of IT investments.

Follow us and join the conversation:

- Twitter
- #IntelIT
- LinkedIn
- IT Center Community

Visit us today at **intel.com/IT** or contact your local Intel representative if you would like to learn more.

Related Content

If you liked this paper, you may also be interested in these related stories:

- Horizontal IoT Platform Paves the Way to Enterprise IoT Success paper
- Improving Manufacturing with Advanced Data Analytics paper
- Intelligent Factories Tap into Data by Connecting the Unconnected paper
- Connecting Legacy Devices to the Internet of Things paper

Printed in USA Please Recycle 0818/SMON/KC/PDF 337117-001US